

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

09/440,467
JUN Yoshida, et al.
11-15-99

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出願年月日
Date of Application:

1998年11月20日

願番号
Application Number:

平成10年特許願第330838号

願人
Applicant(s):

キヤノン株式会社

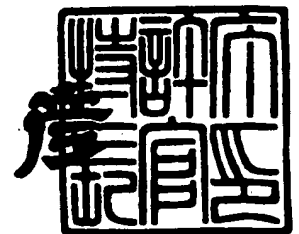


CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年12月10日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特平11-3086974

【書類名】 特許願

【整理番号】 3736019

【提出日】 平成10年11月20日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 電子透かし埋め込み装置、不正検知装置及びコンピュータ読み取り可能な記憶媒体

【請求項の数】 18

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 吉田 淳

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 岩村 恵市

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100090273

 【弁理士】

 【氏名又は名称】 國分 孝悦

 【電話番号】 03-3590-8901

【手数料の表示】

 【予納台帳番号】 035493

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

特平 10-330838

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子透かし埋め込み装置、不正検知装置及びコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項 1】 デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む埋め込み手段と、

上記デジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載するファイル作成手段とを設けたことを特徴とする電子透かし埋め込み装置。

【請求項 2】 デジタルコンテンツの作成時刻を含む電子透かしが埋め込まれたデジタルコンテンツを有すると共にファイル更新時刻が記載されたファイルから上記作成時刻と更新時刻とを抽出する時刻抽出手段と、

上記抽出された作成時刻と更新時刻とを比較する比較手段とを設けたことを特徴とする不正検知装置。

【請求項 3】 デジタルコンテンツに関連する複数の情報を電子透かしとして埋め込む埋め込み手段を設けたことを特徴とする電子透かし埋め込み装置。

【請求項 4】 上記電子透かしは、耐性の弱いものであることを特徴とする請求項 3 記載の電子透かし埋め込み装置。

【請求項 5】 上記複数の関連する情報は、同じ情報であることを特徴とする請求項 3 記載の電子透かし埋め込み装置。

【請求項 6】 上記複数の関連する情報は、異なる情報であることを特徴とする請求項 3 記載の電子透かし埋め込み装置。

【請求項 7】 上記電子透かし埋め込み手段は、それぞれ耐性の異なる複数の電子透かしを埋め込むことを特徴とする請求項 1 記載の電子透かし埋め込み装置。

【請求項 8】 電子透かしが複数の関連する情報と共に埋め込まれたデジタルコンテンツから上記複数の関連する情報を抽出する情報抽出手段と、

上記抽出された複数の情報を比較する比較手段とを設けたことを特徴とする不正検知装置。

【請求項9】 デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む処理と、

上記デジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項10】 デジタルコンテンツの作成時刻を含む電子透かしが埋め込まれたデジタルコンテンツを有すると共にファイル更新時刻が記載されたファイルから上記作成時刻と上記更新時刻とを抽出する処理と、

上記抽出された作成時刻と更新時刻とを比較する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項11】 デジタルコンテンツに複数の関連する情報を電子透かしとして埋め込む処理を実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項12】 上記電子透かしは、耐性の弱いものであることを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項13】 上記複数の関連する情報は、同じ情報であることを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項14】 上記複数の関連する情報は、異なる情報であることを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項15】 上記電子透かしを埋め込む処理は、それぞれ耐性の異なる複数の電子透かしを埋め込むことを特徴とする請求項11記載のコンピュータ読み取り可能な記憶媒体。

【請求項16】 電子透かしが複数の関連する情報と共に埋め込まれたデジタルコンテンツから上記複数の関連する情報を抽出する処理と、

上記抽出された複数の情報を比較する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項17】 デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む処理を実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 18】 電子透かしが埋め込まれたデジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載する処理を実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタルコンテンツに電子透かしを埋め込む電子透かし埋め込み装置、電子透かしが埋め込まれたデジタルコンテンツに対する改竄等の不正を検知する不正検知装置及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【0002】

【従来の技術】

デジタル情報には、従来のアナログ情報と比較し、コンピュータなどによって簡単に劣化すること無くコピー、改竄でき、通信回線を通じて転送することが容易であるという特徴がある。このような特徴により、デジタル情報は安易に不正コピーされ再配布される傾向にあった。

【0003】

これを防ぐための方法の一つとして、電子透かしと呼ばれる手法がある。電子透かしとは、それを埋め込んであるデジタルコンテンツを通常に再生した場合には、人間には知覚できない形で情報を埋め込む手法である。

尚、以下の説明において、デジタルコンテンツとは、動画像、静止画像、音声、コンピュータプログラム及びコンピュータデータ等を指すものとする。

【0004】

電子透かしによる情報埋め込み方式の代表的なものとして、デジタル画像でいえば、画素の色相、明度等にあたる、デジタルコンテンツのデータ値に対し演算を施して電子透かしを埋め込む手法がある。この手法の代表的なものとして、デジタルコンテンツをブロックに分割し、ブロック毎に+1と-1の組み合わせである、予め決められた透かしパターンを足し込むという Digimarc 社、米国特許 5,636,292 号の手法がある。

【0005】

他の電子透かし埋め込み方法の代表的なものとしては、デジタルコンテンツに対し高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより埋め込みを行う手法が挙げられる。

【0006】

高速フーリエ変換による手法では、入力コンテンツは、PN系列を加えられて拡散された後、ブロックに分割される。そして、ブロック毎にフーリエ変換が施され、1ブロックに1ビットの透かし情報が埋め込まれる。透かし情報が埋め込まれたブロックは逆フーリエ変換が施され、再び最初と同じPN系列が加えられて電子透かしが埋め込まれたコンテンツが得られる。この手法は、「大西、岡、松井、”PN系列による画像への透かし署名法”1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26B」に詳しい。

【0007】

離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。1ブロックに1ビットの情報を埋め込んだ後、逆変換をして電子透かし埋め込み済みコンテンツを生成する。この手法は、「中村、小川、高嶋”デジタル画像の著作権保護のための周波数領域における電子透かし方式”1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26A」に詳しい。

【0008】

ウェーブレット変換による手法は、入力コンテンツをブロック分割する必要のない手法であり、「石塚、酒井、櫻井、”ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”1997年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26D」に詳しい。

【0009】

上記のような方法により、デジタルコンテンツに電子透かしとして埋め込まれる情報の代表的なものとして、著作権情報とユーザ情報が挙げられる。著作権情報を埋め込むことにより、ユーザは、デジタルコンテンツに著作権が設定さ

れていることや、著作者は誰であるか等を知ることができる。しかし、実際に著作権が保護されるか否かはユーザのモラルにかかっていた。また、ユーザ情報を埋め込むことにより、不正に再配布されたデジタルコンテンツより、再配布を行ったユーザを検知することができる。しかし、この場合もユーザに対して警告を発する程度の効果しか望めない。

【0010】

今後、インターネット等のインフラがさらに整い、ネットワーク社会が進展するに連れて、デジタルコンテンツがネットワーク上で配信される機会が飛躍的に増加することが予測される。それに伴いより深刻になってくるのが著作権保護に関する問題である。この問題の解決のために、場合によっては著作権の設定されていないデジタルコンテンツも含む全てのデジタルコンテンツに電子透かしが埋め込まれることが一般的になると考えられる。

【0011】

【発明が解決しようとする課題】

しかしながら、上記のように著作権保護のために、従来の方式で電子透かしを埋め込んだ場合においても、著作権が守られるか否かはユーザの意識にかかり、物理的に著作権の保護を行うことはできないという問題があった。

【0012】

本発明は、上記の問題を解決するために成されたもので、デジタルコンテンツに対する不正を検知すること、及びデジタルコンテンツに対してなされた不正を検知し易い電子透かしを埋め込むことができると共に、不正を検知してデジタルコンテンツの著作権を保護することができるようにすることを目的としている。

【0013】

【課題を解決するための手段】

上記の目的を達成するために、本発明による電子透かし埋め込み装置においては、デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む埋め込み手段と、上記デジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載するファイル作成手段とを

設けている。

【0014】

また、本発明による不正検知装置においては、デジタルコンテンツの作成時刻を含む電子透かしが埋め込まれたデジタルコンテンツを有すると共にファイル更新時刻が記載されたファイルから上記作成時刻と更新時刻とを抽出する時刻抽出手段と、上記抽出された作成時刻と更新時刻とを比較する比較手段とを設けている。

【0015】

また、本発明による他の電子透かし埋め込み装置においては、デジタルコンテンツに電子透かしを複数の関連する情報と共に埋め込む埋め込み手段を設けている。

【0016】

また、本発明による他の不正検知装置においては、電子透かしが複数の関連する情報と共に埋め込まれたデジタルコンテンツから上記複数の関連する情報を抽出する情報抽出手段と、上記抽出された情報を比較する比較手段とを設けている。

【0017】

また、本発明による記憶媒体においては、デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む処理と、上記デジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載する処理とを実行するためのプログラムを記憶している。

【0018】

また、本発明による他の記憶媒体においては、デジタルコンテンツの作成時刻を含む電子透かしが埋め込まれたデジタルコンテンツを有すると共にファイル更新時刻が記載されたファイルから上記作成時刻と上記更新時刻とを抽出する処理と、上記抽出された作成時刻と更新時刻とを比較する処理手段とを実行するためのプログラムを記憶している。

【0019】

また、本発明による他の記憶媒体においては、デジタルコンテンツに電子透

かしを複数の関連する情報と共に埋め込む処理を実行するためのプログラムを記憶している。

【0020】

また、本発明による他の記憶媒体においては、電子透かしが複数の関連する情報と共に埋め込まれたデジタルコンテンツから上記複数の関連する情報を抽出する処理と、上記抽出された複数の情報を比較する処理とを実行するためのプログラムを記憶している。

【0021】

また、本発明による他の記憶媒体においては、デジタルコンテンツに、このデジタルコンテンツの作成時刻を含む電子透かしを埋め込む処理を実行するためのプログラムを記憶している。

【0022】

また、本発明による他の記憶媒体においては、電子透かしが埋め込まれたデジタルコンテンツのファイルを作成し、その際、そのファイルにファイル更新時刻を記載する処理を実行するためのプログラムを記憶している。

【0023】

【発明の実施の形態】

以下、本発明の実施の形態を図面と共に説明する。

図1は、一般的なネットワークの構成を示す図であり、本発明の使用環境の一例を示す。公衆ネットワーク101の代表的なものとしてはインターネットが挙げられる。

公衆ネットワーク101には、デジタル画像に代表される様々なデジタルコンテンツを販売、配布する配布サーバ102、警察機関103、ユーザ104、ローカルエリアネットワーク（LAN）105等が接続されている。

【0024】

配布サーバ102は、World Wide Webサーバ（Webサーバ）により構成されるのが一般的である。またLAN105は、ファイアウォール106により外部から遮断され、LAN105—公衆ネットワーク101間では、送信者、送信データの種類など、予め設定されたパラメータを持つ通信のみが許

可されている。

【0025】

また、LAN105内部には、プロキシサーバ107、パーソナルコンピュータ(PC)108、PC108に接続されたディスプレイ109、プリンタ110、また他のPC111、他のPC111に接続されたディスプレイ112、LAN105に直接接続されたプリンタ113等が存在する。プロキシサーバ107は、LAN101内部のPC108、111が、配布サーバ102等のWebサーバにアクセスする際の制御を行っており、両者の間で通信されるデータは全てプロキシサーバ107を通過する。

【0026】

図2は、本実施の形態による著作権保護方式の機能を搭載したプロキシサーバ107の一例を示す図である。

本システムは、システム内の装置間でのデータ交換に使用されるバス201、不正検知装置202、不正検知装置202の検出結果に従って動作する演算処理装置203、I/Oポート204、それぞれの装置を制御するコントローラ205、システムに入力されたデジタルコンテンツを一時的に保存するメモリ206、LAN105等システム外部のネットワークと接続されている通信ポート207、I/Oポート204に接続された外部記憶装置208及びディスプレイ209よりなる。

【0027】

不正検知装置202は、予め電子透かし埋め込み装置によってデジタルコンテンツに埋め込まれた電子透かし情報を検出して、このデジタルコンテンツに対して不正な処理が行われたことを検知する。上記電子透かし埋め込み装置が、デジタルカメラ、スキャナ等の画像入力装置に搭載された場合、この画像入力装置で入力したデジタルコンテンツに対して、不正が行われたことが不正検知装置202で検知可能となる。

【0028】

また、電子透かし埋め込み装置が搭載されたコンピュータ、アプリケーションソフトウェアで、デジタルコンテンツを作成することにより、作成されたディ

デジタルコンテンツに対する不正を不正検知装置202により検知可能である。また、電子透かし埋め込み装置は、記憶装置、配布サーバ、ネットワーク機器等に搭載される場合などがある。

【0029】

本システムにおいて、調査対象となるデジタルコンテンツは、通信ポート207によって、LAN105及び／又はLAN105と公衆ネットワーク101等を通じて読み込まれる。読み込まれたデジタルコンテンツは、メモリ206に一時的に保存される。メモリ206上のデジタルコンテンツは、不正検知装置202に入力され、正当であるか否かが判定される。不正検知装置202でデジタルコンテンツが正当であると判定された場合は、通信ポート207によりデジタルコンテンツの配信依頼を行ったエンティティに対し配信される。

【0030】

また、不正検知装置202で、デジタルコンテンツが不正であると判定された場合は、演算処理装置203により以下のいずれか一つ又は複数の処理が行われる。

- ・演算処理装置203によって、デジタルコンテンツに対してフィルタリング、暗号化、スクランブル、ノイズを加える等の、可視／不可視の電子透かしを埋め込む演算処理を行った後、通信装置207によってデジタルコンテンツの配信依頼を行ったエンティティに出力する。

【0031】

- ・演算処理装置203によって、デジタルコンテンツを入手した入手元の情報、及び／又は読み込みを行ったエンティティの情報、及び／又はデジタルコンテンツの名称等、デジタルコンテンツに関する情報をI/Oポート204に接続された外部記憶装置208及び／又は通信ポート207を経由して配布サーバ102、警察機関103等に存在するデータベースへ書き込む。

【0032】

- ・コントローラ204による制御によって出力を中止する。
- ・演算処理装置203によって、警告メッセージが発生され、I/Oポート204に接続されているディスプレイ209等に警告が表示される。また、通信ポ

ート207によりネットワークを通じ、デジタルコンテンツの入手元、第三者機関に対して警告が発せられるシステムも容易に構成できる。

【0033】

次に、不正検知装置及び電子透かし埋め込み装置をハードウェアで構成した場合の実施の形態について説明する。

不正検知装置及び電子透かし埋め込み装置はハードウェアの他にソフトウェアでも容易に構成可能である。

【0034】

図3は、本発明による電子透かし埋め込み装置の第1の実施の形態を示すブロック図である。

本装置は、デジタルコンテンツが記憶された磁気記憶媒体等の外部記憶媒体301、時計302、ファイル読み取り装置303、埋め込み装置304、ファイル書き込み装置305よりなる。

【0035】

外部記憶媒体301のファイル構成を図4に模式的に示す。

外部記憶媒体301上のファイルは、ディレクトリ領域401とメンバ領域402からなる。ディレクトリ領域401には、記憶されるファイルのファイル名404、メンバ領域402上のファイルの実体の記憶開始アドレス403、ファイルを編集するたびに更新されるファイル更新時刻405、読み取り専用、読み書き可能等のファイルの属性406等がファイル毎に記憶されている。また、メンバ領域402にはファイルの実体407が記憶されている。

【0036】

次に、動作について説明する。

埋め込み装置304では、従来の技術で説明した方法等により電子透かしを埋め込む。電子透かし埋め込みの際に、埋め込み位置を決定するための鍵情報が必要である。埋め込み装置304では、装置内部に保存されている固有の値を鍵情報として電子透かしを埋め込む。

【0037】

尚、電子透かし埋め込み方法として、埋め込み、抽出の際の鍵情報が必要な手

法を用いたが、これは一例であり、他の電子透かし埋め込み方法も使用可能である。

【0038】

また、鍵情報として装置内部に保存されている固有の値を用いたが、装置の外部から入力するなど、他の値も使用可能である。

その場合は、まず、外部記憶装置301のメンバ領域402に保存されているオリジナルのデジタルコンテンツがファイル読み取り装置303により、読みとられ、埋め込み装置304に入力される。埋め込み装置304において、時計装置302からの時刻情報がデジタルコンテンツに埋め込まれ、ファイル書き込み装置305により、外部記憶媒体301のメンバ領域に書き込まれる。

【0039】

これと同時に、外部記憶媒体301のディレクトリ領域401にあるファイル更新時刻が書き込まれる。この時、オリジナルのデジタルコンテンツに透かし埋め込み済みのデジタルコンテンツを上書きした場合、ファイル更新時刻が変更される。

埋め込み装置304が、時刻をデジタルコンテンツに埋め込む際に、安全性を高めるために、暗号化したり、デジタル署名を添付する等の処理を行うことも可能である。

【0040】

本装置により電子透かしが埋め込まれたデジタルコンテンツ（ファイル）を編集すると、電子透かしとして埋め込まれているデジタルコンテンツの作成時刻は変更されないままに、外部記憶媒体301のディレクトリ領域に保存されている最も最後にファイルを変更した時刻であるファイル更新時刻のみが変更されるため、作成時刻とファイル更新時刻との差が、所定のしきい値より大きくなる。

【0041】

ここで、デジタル署名について説明する。デジタル署名とは、メッセージや情報の作成者が確かにそれを作成したことを示すものであり、非対称暗号を用いて実現することが多いが、信頼できる機関があれば対象暗号でも実現可能であ

る。代表的なデジタル署名には、RSA署名、エルガマル署名等がある。

【0042】

RSA署名ではメッセージ（或いはメッセージのハッシュ値）を自分のRSA秘密鍵で暗号化し、それを署名文としてメッセージと共に受信者に送る。受信者は、受け取ったメッセージ（或いはメッセージのハッシュ値）と、署名文を送信者のRSA公開鍵で復号したものを比較し、一致していたら正しい送信者からのメッセージであると判断する。

【0043】

ここで、ハッシュ値について説明する。

ハッシュ値 h とは、ハッシュ関数 $f : x \rightarrow h$ により求められる長い入力列 X の圧縮値である短い出力 h である。また、一方向性関数であり、 $f(x') = f(x)$ を満たす異なる入力 x, x' を求めるのは難しいという性質を持つ。ハッシュ関数の代表的なものとしてMD5 (Message Digest 5)、SHA (Secure Hash Algorithm) 等がある。ハッシュ関数の詳細及びデジタル署名については岡本栄司著「暗号理論入門」（共立出版株式会社）に詳しい。

【0044】

図5は、本発明による不正検知装置の第1の実施の形態を示すブロック図である。

本装置は、外部記憶媒体501、電子透かし抽出装置502及び比較装置503から成る。

【0045】

本装置への入力は、外部記憶媒体501に記憶された調査対象のデジタルコンテンツである。本装置により、正当であるとして出力されるデジタルコンテンツは、図3の電子透かし埋め込み装置によって電子透かしが埋め込まれ、その後、改竄や画像変換等の攻撃等による不正が行われていないデジタルコンテンツである。

【0046】

電子透かし抽出装置502では、電子透かし埋め込み装置304が、埋め込み

の際に行った周波数変換をデジタルコンテンツに対して行う。また、電子透かし抽出装置502は、図3の埋め込み装置304と同様に、装置内部に固有の値が保存されており、固有値の値は、埋め込み装置304の固有値と同じである。

【0047】

電子透かし抽出装置502では、周波数変換処理済みのデジタルコンテンツから固有値を用いて、埋め込まれている情報を抽出する。抽出の方法については、従来の技術で挙げた文献に詳しい。また、上記埋め込み装置304が電子透かしの埋め込みの際に、周波数変換を行わない手法を用いる場合は、電子透かし抽出装置502も周波数変換を行わず、デジタルコンテンツと固有値から情報を抽出する。また、電子透かし埋め込み装置304と同様に、他の抽出方法も使用可能であり、外部から固有値を入力される場合もある。

【0048】

本装置に入力されたデジタルコンテンツは、電子透かし抽出装置502に入力され、電子透かしとして埋め込まれている時刻を読み出し、比較装置503に入力する。比較装置503には、外部記憶媒体501に記録されているファイル更新時刻も入力される。比較装置503では、入力された2つの時刻を比較し、2つの時刻の差が所定のしきい値より大きい場合に、デジタルコンテンツに対して不正が行われたと判定する。

【0049】

次に、電子透かし埋め込み装置及び不正検知装置の第2の実施の形態を説明する。

本実施の形態は、電子透かしの耐性を利用したものであるので、まず、耐性について説明する。

電子透かしを埋め込んだデジタルコンテンツに対してデータ圧縮や、フィルタリング処理を行った際に、電子透かしとして埋め込んだ情報が正しく抽出できるか否かを、電子透かしの耐性と呼ぶ。

【0050】

耐性が強いほど、これらの処理を行った後でも、埋め込まれた情報が残っていることになる。耐性が弱い方法で電子透かしを埋め込んだ場合は、デジタルコ

ンテンツに対して僅かな処理が施されただけで、情報が壊されてしまう可能性が高くなる。

【0051】

図6は、本発明による電子透かし埋め込み装置の第2の実施の形態を示すブロック図である。

本装置は、記憶装置601、埋め込み装置602よりなる。電子透かしを埋め込んだデジタルコンテンツへの改竄が僅かでも、電子透かしが破壊されるほど耐性の弱い埋め込み方法を埋め込み装置602に用いれば、僅かな不正でも検知できる不正検知装置を構成できることになる。また、電子透かしの耐性を向上することによって、デジタルコンテンツへの僅かな不正は許容する不正検知装置を構成できる。

【0052】

本装置への入力は、デジタルコンテンツ、電子透かしとして埋め込む情報列、及びデジタルコンテンツ全体に情報列を電子透かしとして埋め込むための座標値等で表された位置情報である。ここで情報列とは、デジタルコンテンツに固有の情報、電子透かしを埋め込むエンティティの情報、著作権情報、又はデジタルコンテンツを取得するユーザの情報等が符号化されたものである。

【0053】

入力された情報列は、記憶装置601に一時的に記憶された後、埋め込み装置602に埋め込み位置情報と共に入力され、デジタルコンテンツ全体の互いに干渉し合わない位置に繰り返し埋め込まれる。

【0054】

図7は本発明による不正検知装置の第2の実施の形態を示すブロック図である。

本装置は、電子透かし抽出装置701、抽出した情報を記憶する記憶装置702、及び比較装置703よりなる。本装置への入力は、調査対象となるデジタルコンテンツと、電子透かしが埋め込まれている位置を示す座標値等で表された埋め込み位置情報である。

【0055】

本装置より、正当であるとして出力されるデジタルコンテンツは、図6の電子透かし埋め込み装置によって電子透かしが埋め込まれ、その後、改竄等の不正が行われていないデジタルコンテンツである。

【0056】

本装置にデジタルコンテンツ及び埋め込み位置情報が入力されると、電子透かし抽出装置701により、デジタルコンテンツ全体に繰り返し埋め込まれている情報が全て抽出される。この情報は記憶装置702に別個に蓄積された後、比較装置703により比較される。比較装置703では、情報の中に異なっているものがある場合に、そのデジタルコンテンツに対して不正が行われたと判定する。

【0057】

電子透かしは耐性の弱い方法で埋め込まれているので、デジタルコンテンツが改竄等の不正が行われている場合は、埋め込まれている複数の情報のうち、少なくとも1つは破壊されている。

【0058】

ここでは、デジタルコンテンツ全体に同じ情報が埋め込まれているものとしたが、電子透かし埋め込み装置により、異なる情報をデジタルコンテンツ全体に埋め込み、不正検知装置によりそれらの関連性を調べることにより、正当性を検知する装置等を簡単に構成できる。

【0059】

また、図6の電子透かし埋め込み装置において、埋め込み装置602に、埋め込み位置情報と共に、埋め込み位置に対応する量子化ステップを入力することにより、部分的に強度を変えて電子透かしを埋め込むことが可能である。これにより、不正検知装置の抽出装置701に埋め込み位置情報と共に埋め込み位置に対応する量子化ステップを入力し、埋め込み位置に対応する量子化ステップを用いた埋め込み情報の抽出が可能となり、デジタルコンテンツの保護機能の強度を部分的に変えることができる。

【0060】

一例として、埋め込み装置602に適用することのできる埋め込み装置と、対

応する抽出装置の実施の形態を第3の実施の形態として説明する。

図8はデジタルコンテンツへの耐性の弱い電子透かしの埋め込み装置を示すブロック図である。本装置への入力、埋め込み位置情報と、デジタルコンテンツを構成しているデータ値、2進数に符号化されている埋め込み情報であり、電子透かし埋め込み済みのデジタルコンテンツのデータ値が出力される。

【0061】

本装置は、入力されたデータ値を、電子透かしの埋め込み対象になっているデータ値と、なっていないデータ値とに分割するスイッチ801、演算装置802、記憶装置803よりなる。

【0062】

本装置に入力されたデジタルコンテンツのデータ値は、埋め込み位置情報により制御されるスイッチ801によって、埋め込み対象となっているデータ値と、なっていないデータ値とに分割される。埋め込み対象となっているデータ値は、演算装置802に入力され、以下のようにして埋め込み情報が埋め込まれる。

【0063】

まず、データ値の絶対値を所定の数で割る。この時の所定の数を強度、商を量子化ステップと呼ぶ。強度が大きいほど、透かしの耐性が強くなる。次に、各々のデータ値を変更し、量子化ステップと整数の積に一致させる。ここで用いた整数をインデックスと呼ぶ。この時、埋め込み情報が1であったなら、インデックスを奇（偶）数、埋め込み情報が0の場合は、インデックスを偶（奇）数とする。埋め込み情報が埋め込まれたデータ値は、記憶装置803によって、埋め込み対象となっていなかったデータ値と時間的な整合がとられ、出力される。

【0064】

図9は、上記の方法で埋め込まれた電子透かしを抽出する抽出装置の実施の形態を示すブロック図である。

本装置への入力、電子透かしを埋め込まれたデジタルコンテンツ、埋め込み位置情報である。また、本装置はデジタルコンテンツから抽出された埋め込み情報を出力する。

【0065】

入力されたデジタルコンテンツは、埋め込み位置情報により制御されてるスイッチ 901 により、電子透かしが埋め込まれているデータ値と埋め込まれていないデータ値とに分割され、埋め込まれているデータ値は、演算装置 902 に入力される。演算装置 902 では、演算装置 802 と同じ量子化ステップを所有し、それぞれのデータ値のインデックスを調べることにより埋め込まれている情報を摘出し、装置の出力とする。

【0066】

次に、不正検知装置を用いて構成した著作権保護装置のハードウェアでの構成例について説明する。著作権保護装置はハードウェアだけでなく、ソフトウェアでも容易に構成される。

図 10 は不正検知装置を用いて構成したデジタルコンテンツの著作権保護装置の第 1 の実施の形態を示すブロック図である。

【0067】

本装置をディスプレイに搭載した場合は、正当な画像であれば、原画像が表示されるが、不正な画像であれば、フィルタリングされた画像しか表示されない。また、プリンタに搭載した場合は、正当な画像であれば原画像を印字できるが、不正な画像は、フィルタリングされた画像しか印字できない。

【0068】

これによって、例え不正な画像を入手したとしても、実際に利用することは難しいため、著作権保護が実現される。また、プリンタ、ディスプレイに限らず、他のネットワーク構成機器、周辺機器、コンピュータ等にも搭載可能である。

【0069】

本装置は、記憶装置 1001、上記各実施の形態による不正検知装置 1002、不正検知装置 1002 の出力により制御され、デジタルコンテンツを変形し出力するか、そのまま出力するか決定するスイッチ 1003、演算装置 1004 よりなる。

【0070】

本装置に入力されたデジタルコンテンツは、不正検知装置 1002 により、不正であるか否か検査されると共に、記憶装置 1001 に蓄えられる。記憶装置

1001に蓄えられたデジタルコンテンツはスイッチ1003に入力され、不正検知装置1002がデジタルコンテンツは正常であると判定した場合は、そのまま著作権保護装置の出力となり、不正であると判定した場合は、演算装置1004に入力される。

【0071】

デジタルコンテンツは演算装置1004により、フィルタをかけられる等の処理が行われる。デジタルコンテンツが不正であるとされた場合は、このフィルタがかけられたデジタルコンテンツが著作権保護装置の出力となる。ここで、演算装置1004による処理の例としてフィルタリングを挙げたが、スクランブル等の他の処理でもよいことは明らかである。

【0072】

図11は著作権保護装置の第2の実施の形態を示す。

本装置は、特に、入力をデジタル画像に限った場合、図10の演算処理装置1004を、周波数変換装置1104、低域通過フィルタ1105、逆周波数変換装置1106で置き換えることにより、不正が検知された場合に、デジタル画像を低解像度化して出力するようにしたものである。

【0073】

例えば本装置をディスプレイに搭載した場合は、正当な画像であれば高解像度で見ることができるが、不正な画像であれば低解像度でしか見ることができない。また、プリンタに搭載した場合は、正規画像は高解像度で印字できるが、不正画像は低解像度でしか印字できないプリンタを構成できる。

【0074】

図11において、不正検知装置1002が、入力されたデジタル画像を不正であると判定した場合は、記憶装置1001に記憶されているデジタル画像は、周波数変換装置1104により周波数領域に変換され、低域通過フィルタ1105により、高域がカットされ、逆周波数変換装置1106により空間領域に戻される。この一連の操作により、デジタル画像は圧縮されるため、著作権保護機能を実現できる。

【0075】

図12は著作権保護装置の第3の実施の形態を示すもので、図10の演算装置1004に代えて暗号化装置1204を用いることにより、不正を検知した場合に、入力されたデジタルコンテンツを暗号化して出力するようにしたものである。

例えばこの著作権保護装置をハードディスク等に搭載することにより、図1の配布サーバ102より、不正であるか否かに関わらず、誰でもデジタルコンテンツをダウンロードし、保存することができるが、不正なデジタル画像であれば、保存は暗号化された状態で行われるので、保存されたデータは正しい復号鍵を持ってしか読むことはできない。著作権保護のために本装置を用いることを考慮すると、復号鍵は、例えば警察等公平な立場の第三者が所有するのが適切である。

【0076】

図12において、不正検知装置1002が、入力されたデジタルコンテンツを不正であると判定した場合は、記憶装置1001に記憶されているデジタルコンテンツは暗号化装置1204により、暗号化された後、出力される。これにより、著作権保護機能を実現できる。ここで用いられる暗号化には、DES等の共通鍵暗号化方式、RSA等の公開鍵暗号化方式が用いられる（各暗号の詳細は、岡本栄司著「暗号理論入門」共立出版株式会社参照）。

【0077】

図13は著作権保護装置の第4の実施の形態を示すもので、上記演算装置1004に代えて加算装置1304を用いることにより、入力されたデジタルコンテンツの不正が検知された場合、入力されたデジタルコンテンツにノイズを加えて出力するようにしたものである。

【0078】

本装置は、ディスプレイ、プリンタ等の出力装置への搭載が効果的である。改竄されたデジタルコンテンツが入力された場合、本装置を搭載した出力装置の出力は、ノイズの乗ったデジタルコンテンツとなる。尚、ディスプレイ、プリンタ以外の他の機器にも搭載できることは明らかである。

【0079】

図 13 において、不正検知装置 1002 がデジタルコンテンツを不正であると判定した場合は、記憶装置 1001 に蓄えられたデジタルコンテンツは、加算装置 1304 にビット列と共に入力され、加算され出力される。これにより、デジタルコンテンツにノイズが加えられ、使用するのに適さない品質にすることができる。ここで加えられるビット列は、ランダムなノイズ、規則性のあるノイズの他、意味のある情報を表していてもよい。これにより、著作権保護機能を実現できる。

【0080】

図 14 は著作権保護装置の第 5 の実施の形態を示すもので、上記演算装置 1004 に代えて透かし埋め込み装置 1404 を用いることにより、不正なデジタルコンテンツには電子透かしを埋め込んで出力するようにしたものである。

【0081】

透かし埋め込み装置 1404 により、可視型の電子透かしを埋め込むようにすれば、著作権保護装置をプリンタ、ディスプレイ等の出力装置に搭載することにより、デジタルコンテンツの不正検知時に、デジタルコンテンツ上に文字やマーク等を構成した画像が出力される。

【0082】

また、不可視型の電子透かしを埋め込むようにすれば、外部記憶装置等に搭載することにより、電子透かしとして、デジタルコンテンツの入手者情報、入手元情報が埋め込まれる。これにより、不正な画像に関わらない限り、上記情報はデジタルコンテンツに埋め込まれることはないため、プライバシーが保護され、また、不正な画像に関わった場合には、上記情報が埋め込まれることにより、警察等の捜査を可能とし、プライバシーが保護される。

尚、プリンタ、ディスプレイ、外部記憶機器以外の他の機器にも搭載可能であることは明らかである。

【0083】

図 14 において、入力されたデジタルコンテンツを不正であると判定した場合は、不正検知装置 1002 が記憶装置 1001 に蓄えられたデジタルコンテンツは、埋め込み情報と共に透かし埋め込み装置 1404 に入力される。電子透

かし埋め込み装置 1404 では、デジタルコンテンツに電子透かしを埋め込む。これにより、著作権保護機能を実現できる。

【0084】

図 15 は著作権保護装置の第 6 の実施の形態を示すものである。

本装置は、不正検知装置 1501、不正検知装置 1501 の出力に制御されるスイッチ 1502、デジタルコンテンツに対して不正を行ったユーザのユーザ情報を記憶するデータベース 1503 よりなる。

本装置への入力は、調査対象であるデジタルコンテンツ及びデジタルコンテンツを入手した入手元のユーザ情報である。

【0085】

本装置にデジタルコンテンツが入力されると、不正検知装置 1501 によりデジタルコンテンツが不正であるかどうか検査される。不正検知装置 1501 の出力はスイッチ 1502 に入力され、デジタルコンテンツが不正である場合、スイッチ 1502 により、デジタルコンテンツの入手元情報がデータベース 1503 に入力され記憶される。正当である場合は、入手元情報は記憶されない。

【0086】

データベース 1503 は、配布サーバ、警察機関等に存在し、ネットワークを通じて書き込まれることが妥当である。データベース 1503 に書き込まれたデータは、犯罪捜査時等に警察機関等によって利用される。

また、データベース 1503 に書き込まれるデータとして、上記入手元ユーザ情報の他、入手ユーザ情報、著作権情報、デジタルコンテンツの名称等が有効である。

【0087】

図 16 は著作権保護装置の第 7 の実施の形態を示すブロック図である。

本装置は、入力されたデジタルコンテンツが正当であるものと認められたときに、入力されたデジタルコンテンツを出力し、それ以外の場合には、何も出力しない。即ち、本装置をプリンタに搭載した場合、不正な画像の印字を試みた場合は、何も出力されない。またディスプレイに搭載した場合は、不正な画像は

表示されず、記憶装置に搭載した場合は、不正なデジタルデータは記憶されない。

【0088】

本装置は、不正検知装置1601と、不正検知装置1601により制御されるスイッチ1602よりなる。本装置に入力されたデジタルコンテンツは、不正検知装置1601とスイッチ1602に入力され、不正検知装置1601がデジタルコンテンツが正当であると判定したときのみ、スイッチ1602が出力側に切り替わり、デジタルコンテンツが出力される。

【0089】

本実施の形態では、デジタルコンテンツの全部を出力しない装置を構成したが、デジタルコンテンツの一部を出力しない装置、例えば、カラーデジタル画像を出力する装置で、画像の内、輝度や明度、R、G、B等の任意のパラメータを出力しない装置も容易に構成することができる。

【0090】

図17は著作権保護装置の第8の実施の形態を示ブロック図である。

本装置は、入力されたデジタルコンテンツが不正であると認められたときに、警告を出力するものである。本装置は、PC、ディスプレイ、プリンタ等に搭載され、画像を利用しようとしたユーザに対し警告を発する他、図1のプロキシサーバ107、ファイアウォール106、、配布サーバ102等にも搭載可能である。これらに搭載された場合、不正コンテンツを配布したユーザ、警察、配布サーバ等のオペレータに対して、ネットワークを通じ警告を発することも可能となる。

【0091】

本装置は、不正検知装置1701と、不正検知装置1701により制御される警告発生装置1702からなる。本装置に入力されたデジタルコンテンツは、不正検知装置1701に入力され、デジタルコンテンツが不正であるか否かを検知される。不正である場合は、警告発生装置1702により、上記警告先に警告する。デジタルコンテンツが正当であった場合は、何も行わない。

【0092】

尚、以上の各実施の形態による著作権保護装置を複数組み合わせることで、著作権保護機能を多重に有する著作権保護装置を構成することができる。

また、各実施の形態による不正検知装置、電子透かし埋め込み装置を複数組み合わせることにより、様々な不正検知装置、電子透かし埋め込み装置を構成することができる。

【0093】

次に本発明の他の実施の形態としての記憶媒体について説明する。

本発明はハードウェアで構成することもできるが、CPUとメモリとで構成されるコンピュータシステムで構成することもできる。コンピュータシステムで構成する場合、上記メモリは本発明による記憶媒体を構成する。即ち、前述した各実施の形態で説明した動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のCPUが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【0094】

また、この記憶媒体としては、ROM、RAM等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをCD-ROM、フロッピーディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【0095】

従って、この記憶媒体を各図に示したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【0096】

また、コンピュータ上で稼働しているOS等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入

された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるCPU等が処理の一部又は全部を行う場合にも、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができる。本発明の目的を達成することができる。

【0097】

【発明の効果】

以上説明したように、本発明による電子透かし埋め込み装置及びその関連する記憶媒体によれば、デジタルコンテンツに対して何らかの不正がなされても、あとで不正を検知し易い電子透かしをデジタルコンテンツに埋め込むことができる。

【0098】

また、本発明による不正検知装置及びその関連する記憶媒体によれば、上記電子透かし埋め込み装置で埋め込まれたデジタルコンテンツから抽出された電子透かしに基づいて、そのデジタルコンテンツに対して何らかの不正があったことを容易に検知することができる。

【図面の簡単な説明】

【図1】

一般的な公衆ネットワークと公衆ネットワークにつながる機器の構成図である。

【図2】

著作権保護方式の機能を搭載したネットワークの構成図である。

【図3】

本発明による電子透かし埋め込み装置の第1の実施の形態を示すブロック図である。

【図4】

外部記憶媒体のファイル構成を概念的に示す構成図である。

【図5】

本発明による不正検知装置の第1の実施の形態を示すブロック図である。

【図 6】

本発明による電子透かし埋め込み装置の第 2 の実施の形態を示すブロック図である。

【図 7】

本発明による不正検知装置の第 2 の実施の形態を示すブロック図である。

【図 8】

本発明による電子透かし埋め込み装置の第 3 の実施の形態を示すブロック図である。

【図 9】

本発明による不正検知装置の第 3 の実施の形態を示すブロック図である。

【図 10】

不正検知装置を用いた著作権保護装置の第 1 の実施の形態を示すブロック図である。

【図 11】

著作権保護装置の第 2 の実施の形態を示すブロック図である。

【図 12】

著作権保護装置の第 3 の実施の形態を示すブロック図である。

【図 13】

著作権保護装置の第 4 の実施の形態を示すブロック図である。

【図 14】

著作権保護装置の第 5 の実施の形態を示すブロック図である。

【図 15】

著作権保護装置の第 6 の実施の形態を示すブロック図である。

【図 16】

著作権保護装置の第 7 の実施の形態を示すブロック図である。

【図 17】

著作権保護装置の第 8 の実施の形態を示すブロック図である。

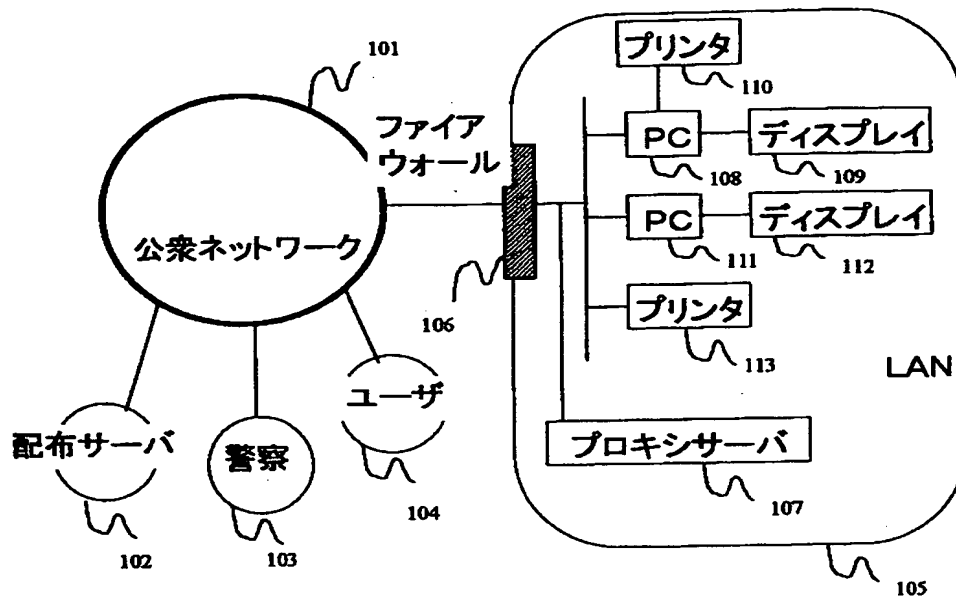
【符号の説明】

202 不正検知装置

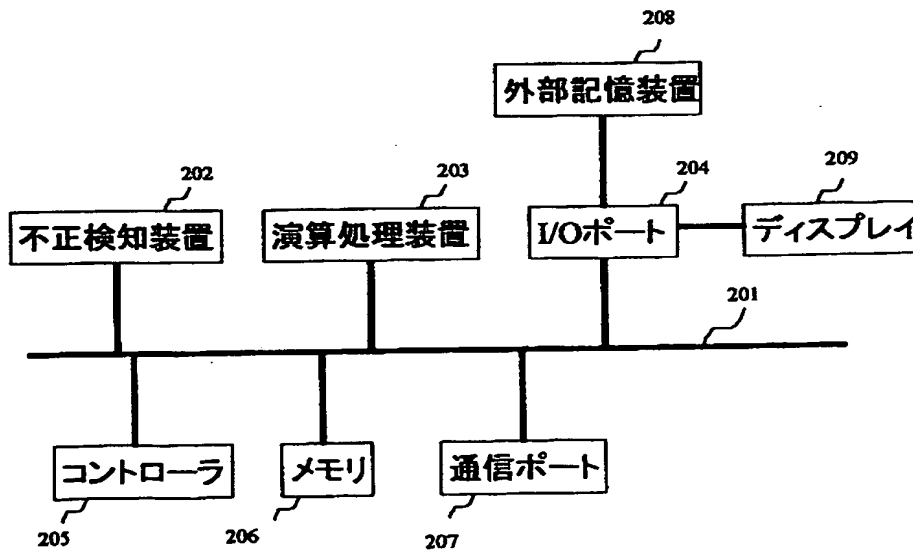
203 演算処理装置
205 コントローラ
208 外部記憶装置
301、401、501 外部記憶媒体
302 時計
303 ファイル読み取り装置
304、602 埋め込み装置
305 ファイル書き込み装置
502、701 抽出装置
503、703 比較装置
601、702、803 記憶装置
801、901 スイッチ
802、902 演算装置

【書類名】 図面

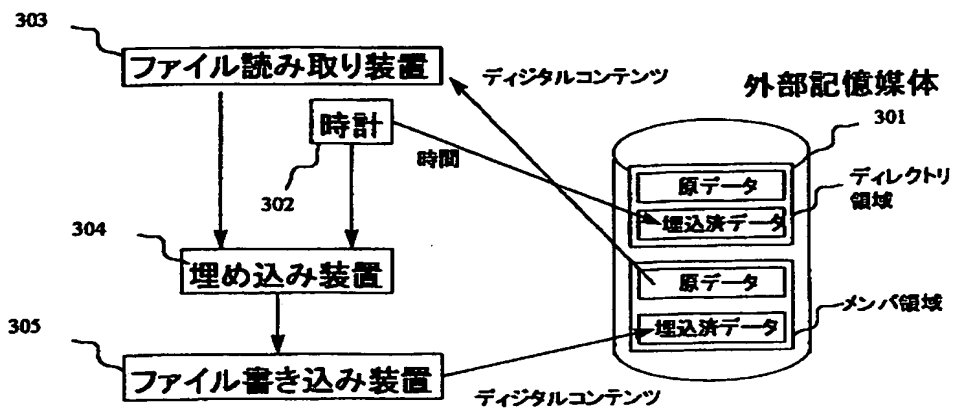
【図 1】



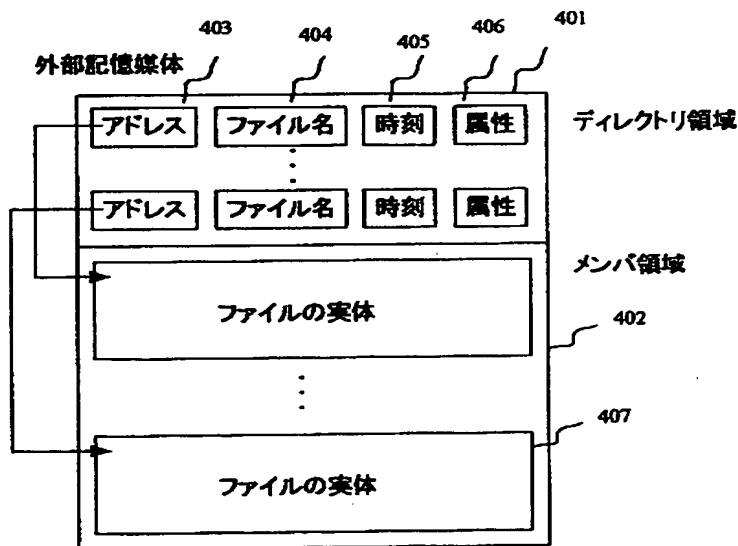
【図 2】



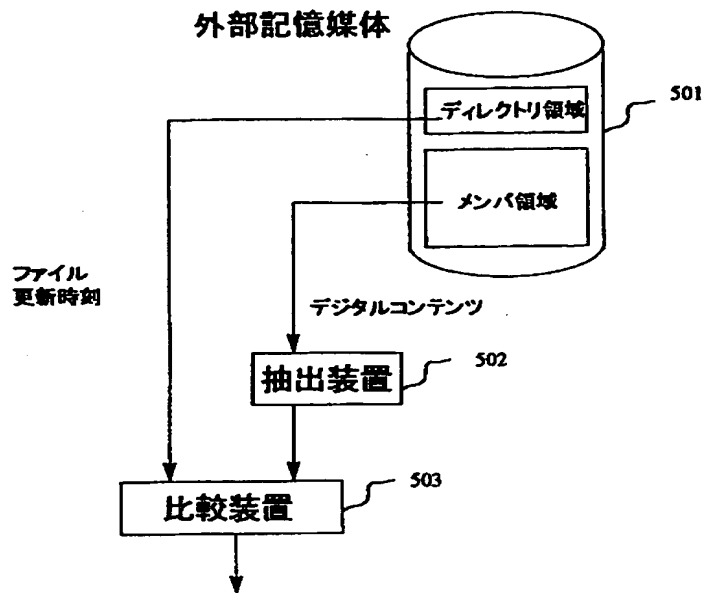
【図 3】



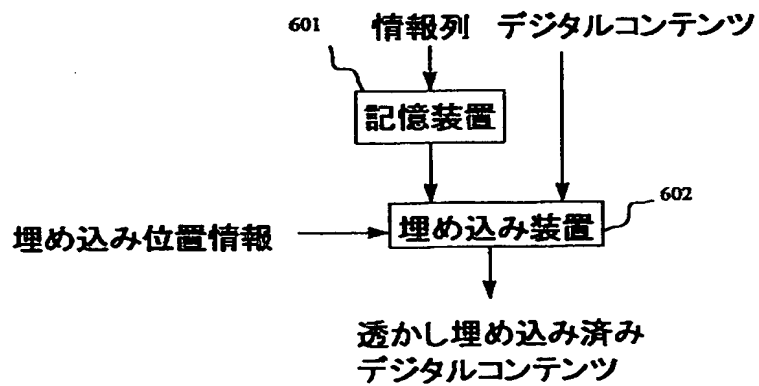
【図 4】



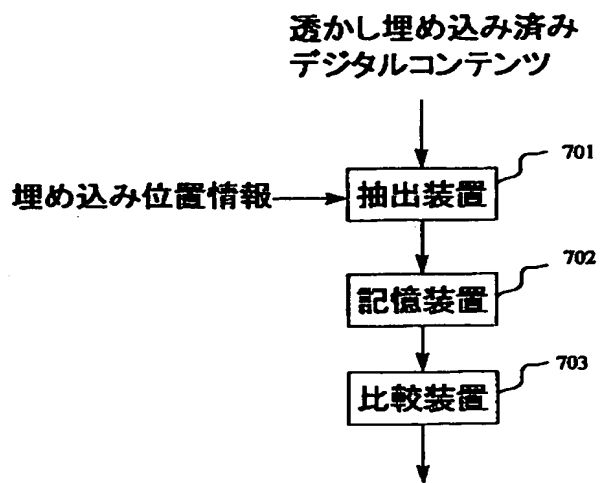
【図 5】



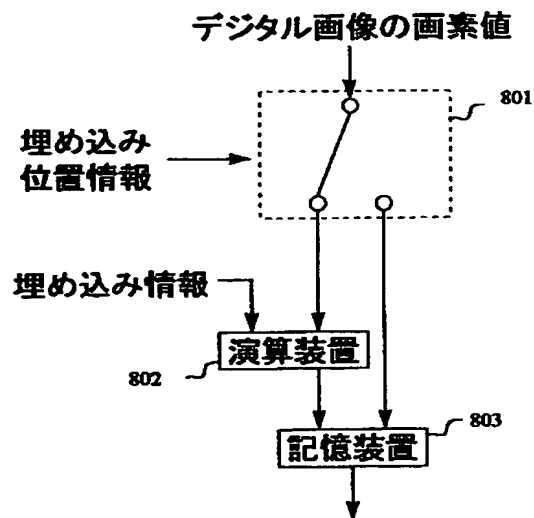
【図 6】



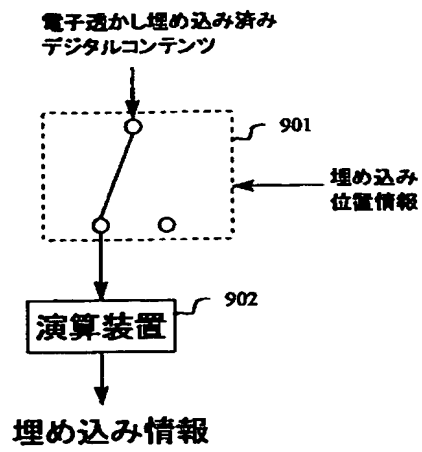
【図 7】



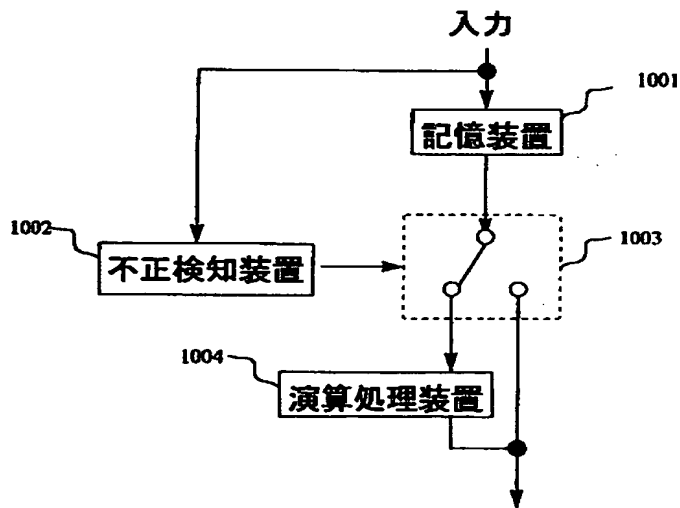
【図 8】



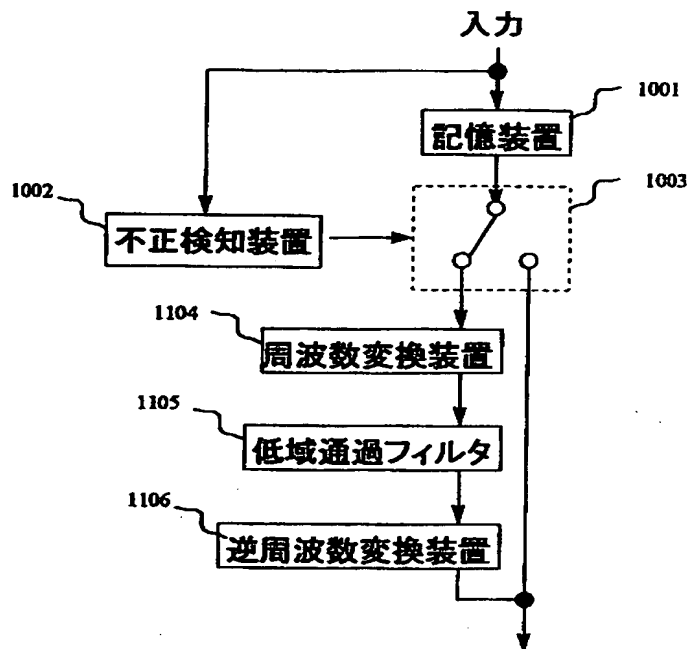
【図 9】



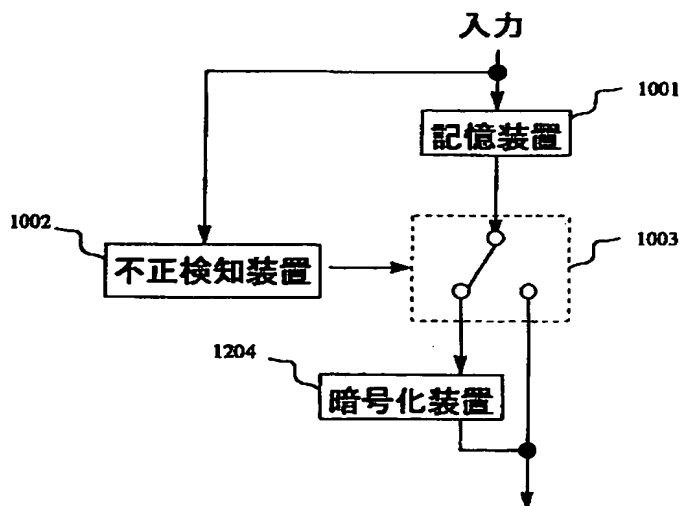
【図 10】



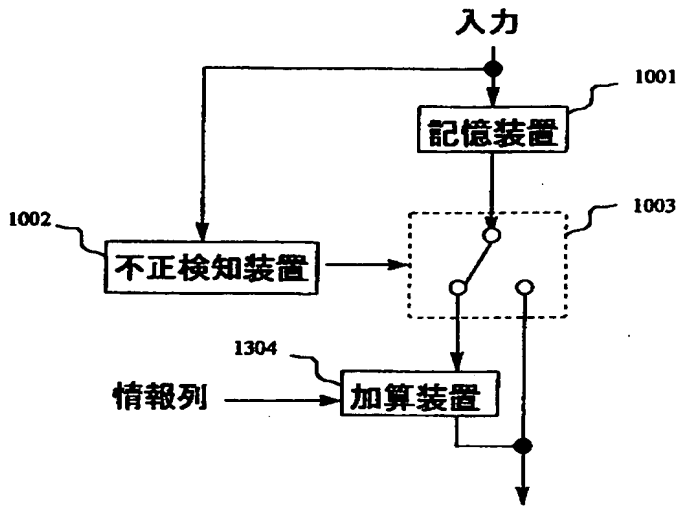
【図 11】



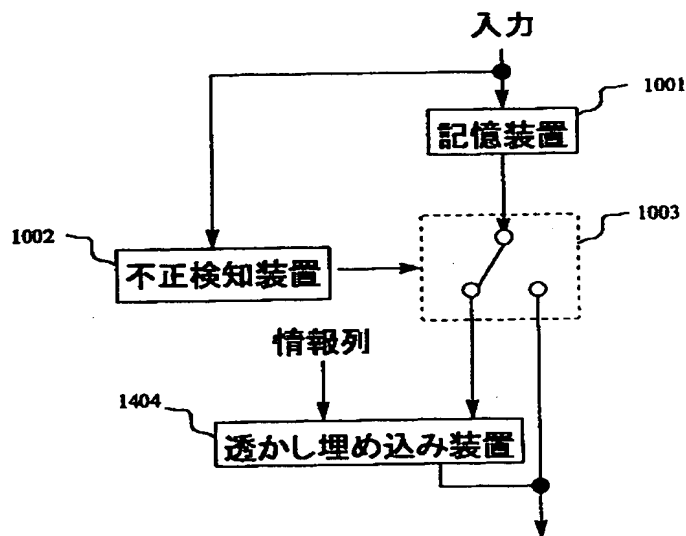
【図 12】



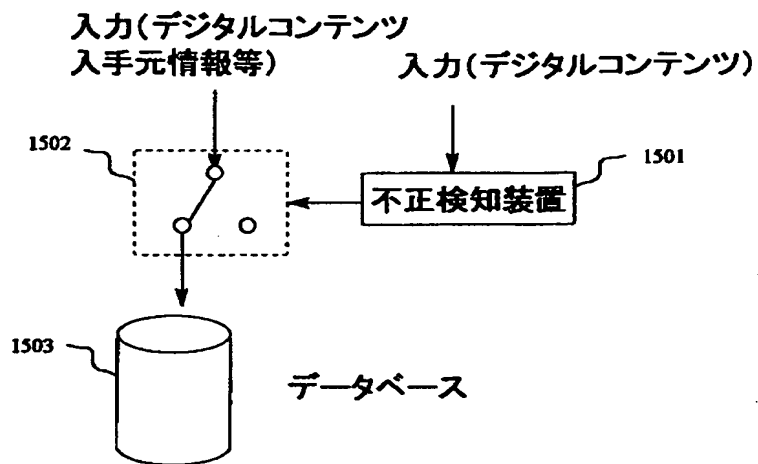
【図 13】



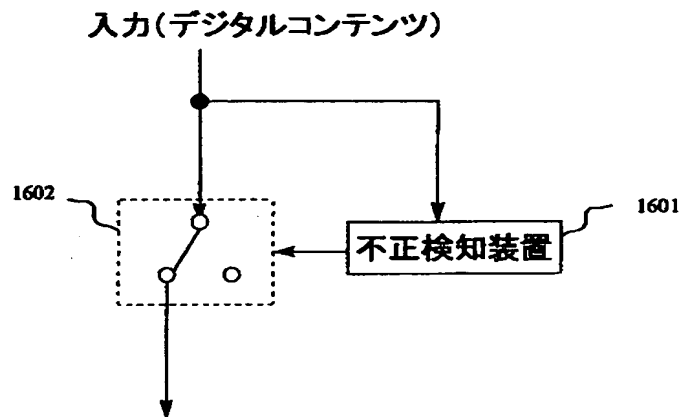
【図 14】



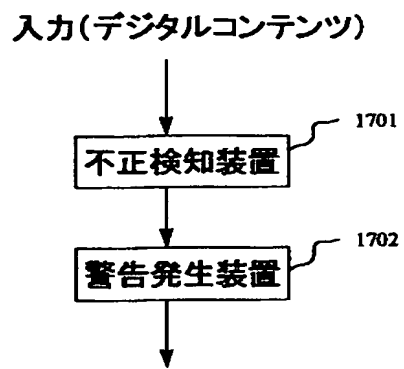
【図 15】



【図 16】



【図 17】



【書類名】 要約書

【要約】

【課題】 デジタルコンテンツに対して改竄等の不正が成された場合に、その不正を検知し易い電子透かしをデジタルコンテンツに埋め込む。

【解決手段】 外部記憶媒体 301 から画像等の原デジタルコンテンツのファイルを読み出し、埋め込み装置 304 において、上記読み出したデジタルコンテンツに対してその作成時刻を含む電子透かしを埋め込むと共に、そのファイルの更新時刻を時計 302 から得て、そのファイルに記載する。再生時には、上記ファイルから上記作成時刻と更新時刻とを抽出して比較し、その差が所定より大きいとき、不正があったものとする。

【選択図】 図 3

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キヤノン株式会社

【代理人】 申請人

【識別番号】 100090273

【住所又は居所】 東京都豊島区東池袋1丁目17番8号 池袋TGホ
ーメストビル5階 國分特許事務所

【氏名又は名称】 國分 孝悦

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号

氏 名 キヤノン株式会社